## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A computer implemented system that facilitates ~~enabling~~ an application to produce a response to an authentication challenge, comprising:

an authentication manager ~~adapted to~~ that receives ~~a~~ first data associated with the communication challenge and ~~to~~ processes the first data into [[a]] second data of a first type appropriate for a first authentication module, the authentication manager further processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for the secondary data, the authentication manager further ~~operable to~~ communicates at least one of the secondary data to at least one authentication module, the at least one secondary data is related to the first data and the authentication challenge; and

at least one authentication module ~~adapted to~~ that receives the at least one ~~the~~ secondary data from the authentication manager and ~~to~~ produces [[a]] third data related to responding to the authentication challenge.

2. (Currently Amended) The system of claim 1, comprising a cache ~~adapted to~~ that stores one or more third data related to responding to the authentication challenge.

3. (Currently Amended) The system of claim 2 [[1]], wherein the authentication manager ~~is further adapted to~~ receives a set of first data associated with a multipart authentication challenge, to process the set of first data into a set of the secondary data, and ~~to~~ communicates the set of secondary data to at least one authentication module, the set of secondary data is related to the set of first data and the multipart authentication challenge.

4. (Currently Amended) The system of claim 3, wherein the at least one authentication module ~~is further adapted to~~ receives [[a]] the set of secondary data from the authentication

manager and ~~to~~ produces a set of third data related to responding to the multipart authentication challenge.

5. (Currently Amended) The system of claim 4, wherein the cache ~~is further adapted to~~ stores a set of third data related to responding to the multipart authentication challenge.

6. (Currently Amended) The system of claim 2, wherein:

the authentication manager ~~is further adapted to~~ accepts a pre-authentication challenge test message associated with an anticipated communication challenge, ~~to~~ processes the test message into a ~~fourth~~ pre-authentication challenge test data, and ~~to~~ communicates the ~~fourth~~ pre-authentication challenge test data to at least one authentication module, the ~~fourth~~ pre-authentication challenge test data related to the pre-authentication challenge test message;

at least one authentication module ~~is further adapted to~~ receives the ~~fourth~~ pre-authentication challenge test data from the authentication manager and ~~to~~ produces a ~~fifth~~ pre-authentication challenge test response data related to responding to the pre-authentication challenge test message; and

the cache ~~is further adapted to~~ stores one or more ~~fifth~~ pre-authentication challenge test response data related to responding to the pre-authentication challenge test message, the cache ~~operable to~~ selectively provides the ~~fifth~~ pre-authentication challenge test response data upon request by the authentication manager.

7. (Currently Amended) The system of claim 6, wherein the authentication modules ~~are further adapted to pass a sixth data to~~ employ one or more services~~, the services employed to facilitate producing the third data~~.

8. (Currently Amended) The system of claim 1, comprising:

a class factory, the class factory ~~operable to~~ selectively instantiates one or more authentication objects based, at least in part, on the first data, and

the class factory ~~operable to~~ makes the one or more instantiated authentication objects callable by the authentication manager.

9. (Currently Amended) The system of claim 8, comprising:

a data store ~~operable to~~ that holds information associated with selectively instantiating the one or more authentication objects, the data store further ~~operable to~~ holds information associated with making the one or more instantiated authentication objects callable by the authentication manager.

10. (Currently Amended) The system of claim 9, comprising:

a registrar ~~adapted to~~ that registers an authentication object with the class factory.

11. (Currently Amended) The system of claim 10, wherein the registrar ~~is further adapted to~~ registers an authentication object with the data store.

12. (Currently Amended) The system of claim 11, wherein the application does not have to be recoded or recompiled to employ the ~~newly~~ registered authentication object.

13. (Currently Amended) The system of claim 1, wherein one or more authentication objects ~~are operable to~~ generate the third data associated with responding to an authentication challenge associated with at least one of, a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

14. (Currently Amended) The system of claim 1, wherein the authentication manager and the one or more authentication objects are distributed to one or more ~~distributed processors~~ computers.

15. (Currently Amended) The system of claim 11, wherein the class factory, the data store and the registrar are distributed to one or more ~~distributed processors~~ computers.

16. (Currently Amended) A computer implemented method for enabling an application to produce a response to an authentication challenge, comprising:

employing a component implemented on a computer readable medium to accepting an authentication challenge;

passing a first data associated with the authentication challenge to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for the secondary data ~~is operable to pass data to one or more authentication modules~~;

passing at least one of the ~~a~~ secondary data associated with the authentication challenge to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager; and

producing one or more responses to the authentication challenge.

17. (Original) The system of claim 16, comprising:

caching one or more responses to the authentication challenge; and

retrieving a response from the cached responses.

18. (Original) The method of claim 16, wherein the authentication challenge is generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

19. (Original) The method of claim 16, wherein one or more authentication modules can be created and registered after the receipt of one or more authentication challenges.

20. (Currently Amended) A computer readable medium, comprising:

computer executable instructions ~~operable to~~ that perform the method of claim 19 ~~16~~.

21. (Cancelled).

22. (Currently Amended) A computer implemented method for enabling an application to produce a response to an authentication challenge, comprising:

generating a pre-authentication challenge test message;

utilizing a component implemented on a computer readable medium to passing a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for secondary data ~~is operable to pass data to one or more authentication modules~~;

passing at least one of the ~~a~~ secondary data associated with the pre-authentication challenge test message to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;

producing one or more responses to the pre-authentication challenge test message; and

caching the one or more responses to the pre-authentication challenge test message.

23. (Original) The method of claim 22, wherein the pre-authentication challenge test message is related to an authentication challenge generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

24. (Original) The method of claim 22, wherein one or more authentication modules can be created and registered after the generation of one or more pre-authentication challenge test messages.

25. (Currently Amended) The method of claim 22, wherein the application does not have to be recoded or recompiled to employ the ~~newly~~ one or more created and registered authentication modules.

26. (Currently Amended) A computer readable medium having computer executable instructions operable to perform a method comprising:

generating a pre-authentication challenge test message;

passing a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager processes the first data into second data of a first type appropriate for a first authentication module, further where the authentication manager processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for secondary data, ~~is operable to pass data to one or more authentication modules~~;

employing a component implemented on a computer readable medium to pass~~ing~~ at least one of the ~~a~~ secondary data associated with the pre-authentication challenge test message to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;

producing one or more responses to the pre-authentication challenge test message; and

caching the one or more responses to the pre-authentication challenge test message.

27. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to selecting an authentication object to process data associated with an authentication challenge.

28. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to registering an authentication object with a class factory and a data store, wherein registering the authentication object facilitates an authentication manager employing the authentication object to produce a response to an authentication challenge.

29. (Withdrawn) A data packet adapted to be transmitted between two or more computer processes, the data packet containing a response to an authentication challenge, where the response was generated by an authentication module adapted to receive data from an authentication manager and to send the response to the authentication manager.

30. (Currently Amended) A system enabling an application to respond to a challenge to a request to access a resource addressable by a URI, comprising:

receiving means for receiving a challenge, the receiving means separate from the application;

distributing means for processing data associated with the challenge into second data of a first type appropriate for a first authentication module and second data of a second type appropriate for a second authentication module and distributing at least one of the secondary data ~~challenge~~ to one or more producing means, the distributing means being separate from the application, the first and second authentication modules having different requirements for secondary data;

producing means for producing a response to the challenge; the producing means being separate from the application; and

storing means for storing a response to the challenge.